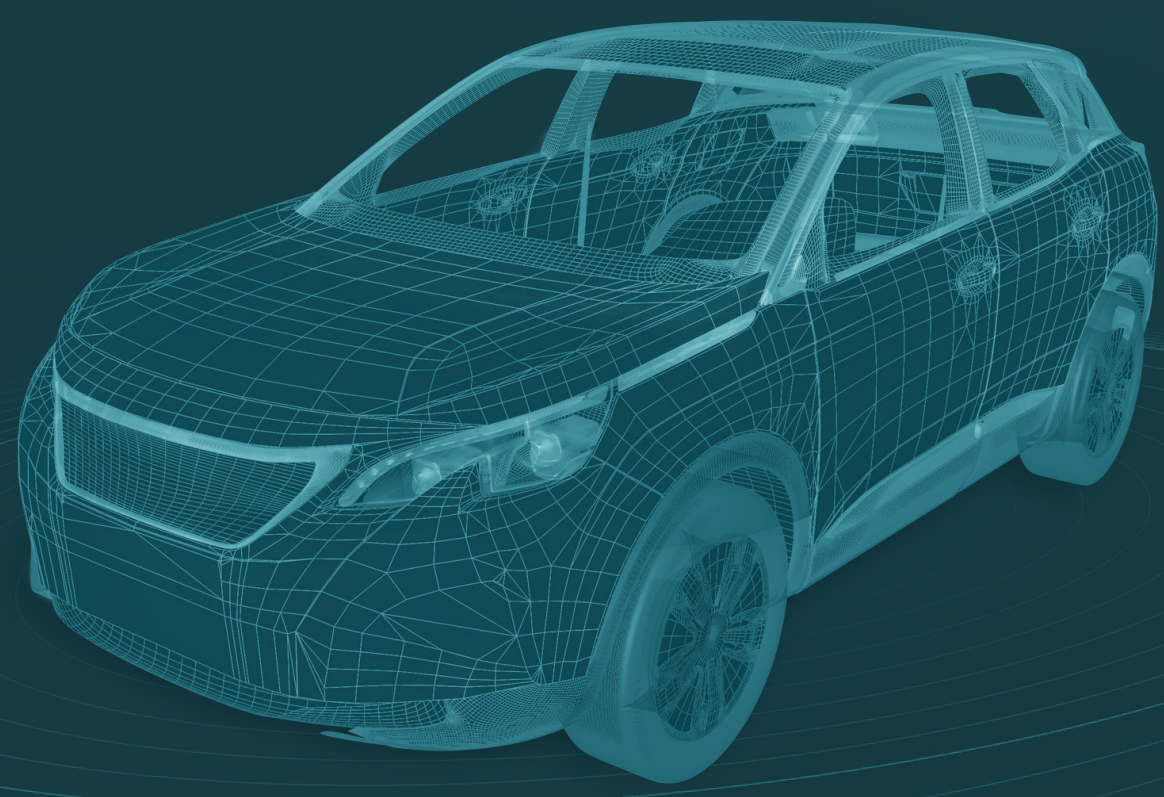
C2A security

STATE OF THE INDUSTRY REPORT

CYBERSECURITY LIFECYCLE MANAGEMENT FOR MODERN VEHICLES

An automotive industry report analyzing current approaches to cybersecurity lifecycle management processes, and how to improve them



September 2020

Conducted by C2A Security

TABLE OF CONTENTS

All rights reserved

ABSTRACT

As the automotive industry copes with a seismic shift towards modern vehicle architecture, OEMs, Tier-1s and other automotive industry suppliers are struggling to adapt. Consumer demand for newer, more connected vehicles with advanced driver assist, and in some cases, autonomous features mean that OEMs are developing more car models with more complex systems architecture. The components required from a variety of sources compromise the automotive supply chain, complicating the planning and implementation of cybersecurity measures. Both within OEMs and Tier-1s and down the supply chain, different internal and external teams are responsible for different tasks in the vehicle lifecycle, and struggle to communicate and coordinate, leading to ineffective task management and assignment. At present, there is no harmonized means of cybersecurity communication or project management - meaning that most elemental and repetitive tasks, like risk assessment, are more complicated and time consuming than ever before.

To further complicate matters, OEMs, Tier-1s and other automotive industry suppliers are on a tight schedule to incorporate the new ISO 21434 standard and UNECE WP.29 regulation that set basic guidelines for cybersecurity management systems. These regulatory activities define the categoric directive for implementing cybersecurity management systems for the protection of vehicles. The regulation outlines key considerations for proper cybersecurity lifecycle management for the vehicle, from risk assessment and product design to when the vehicle is on the road. The new regulation activities indicate a positive development for automotive cybersecurity: stakeholders are prioritizing cybersecurity as a safety issue in a way that they have not before and are acknowledging that vehicle architecture must be secure against attacks to mitigate risks to the public.

”

Most elemental and repetitive tasks, like risk assessment, are more complicated and time consuming than ever before.

”

OEMs, Tier-1s and other automotive industry suppliers are on a tight schedule to incorporate new ISO 21434 standard and UNECE WP.29 regulation.

All rights reserved

In the midst of these ongoing challenges, OEMs and Tier-1s must now adopt new approaches to tackling cybersecurity lifecycle management challenges while adhering to regulation. In this new reality, automotive manufacturers need to operate and account for a variety of cybersecurity activities with different internal and external teams throughout the vehicle lifecycle. There is much to be learned in this adoption process, and the industry can improve and adapt more quickly with a strong understanding of where strengths and weaknesses lie in the cybersecurity lifecycle management process. To this end, C2A Security, a trusted automotive industry cybersecurity solutions provider, has conducted a confidential cybersecurity lifecycle management survey with OEMs and Tier-1s.

”

OEMs and Tier-1s must now adopt new approaches to tackling cybersecurity lifecycle management challenges while adhering to regulation.

The Survey

Survey results are focused on the current state of ongoing automotive cybersecurity management processes, and the preparedness of the automotive industry for the implementation of ISO 21434 standard. The anonymous survey posed key questions about cybersecurity lifecycle management processes within different organizations to professionals across the automotive industry and associated supply chains.

With the results of this survey, the hope is that the information will be used to foster collaboration amongst OEMs, suppliers and technology providers with a clearer understanding of the strengths and weaknesses in industry cybersecurity processes. Armed with this information, the industry can learn what tools are needed to build a more integrated, comprehensive approach to cybersecurity lifecycle management in a way that protects consumers and manufacturers from cybersecurity risk.

All rights reserved

FINDINGS

Assessing the Industry's Current Approach to Cybersecurity Lifecycle Management

VISIBILITY AND TRANSPARENCY

Visibility is the foundation for cyber resilience - here's where the industry is now

Visibility is not only key to effective cybersecurity lifecycle management, but is the foundation for cyber resilience, allowing for complete control throughout the cybersecurity management process. While the industry does have some visibility into the vehicle lifecycle, there is room for improvement. When asked about visibility and insight, the survey results supported these claims: **40%** of participants acknowledge they do not have complete hardware and software bills of materials (BOMs) visibility for their car models to be released next year. Furthermore, **more than half** of survey participants testify that they do not have traceability from software and hardware BOM to vehicle identification number (VIN) for vehicles on the road today.

Fig A.

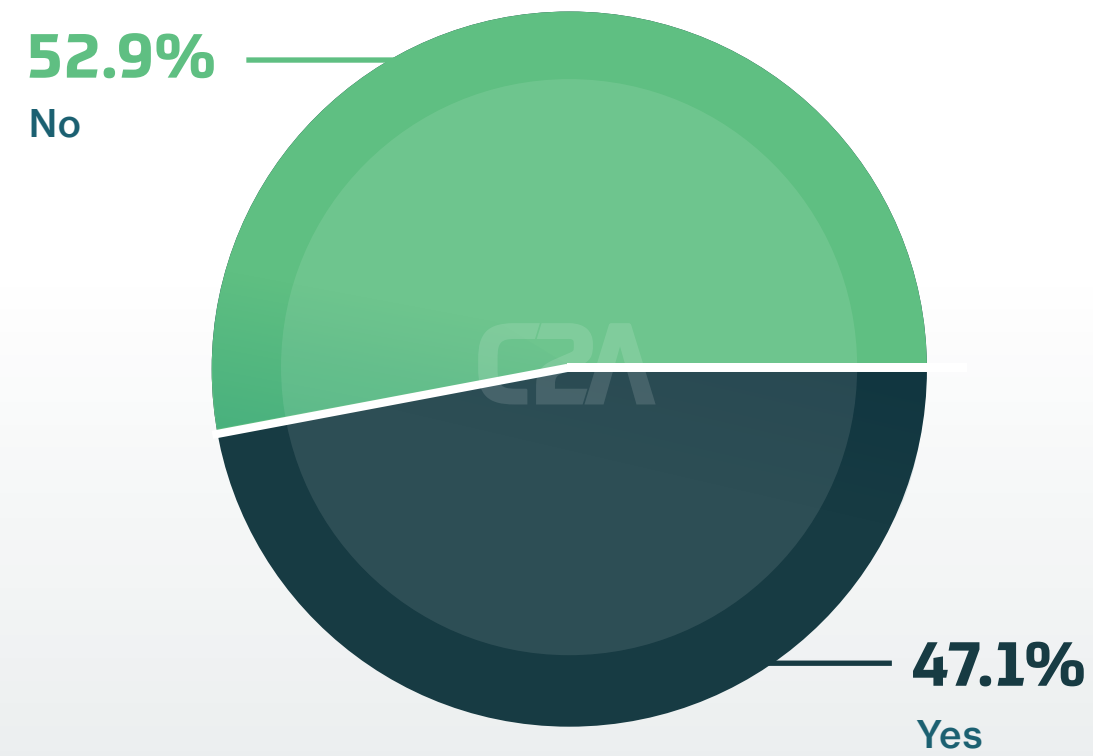
QUESTION:

Do you have traceability from SW & HW BOM to VIN (which vehicle on the road has what HW/SW per ECU)?

Over

50%

of participants testified they do not have traceability



All rights reserved

So the industry lacks visibility. What does this mean for vehicles?

Without absolute visibility, there could be confusion among internal and external teams, and imprecise cybersecurity practices. Though there is slight improvement from vehicles being rolled out from 2021 onwards, the industry has clearly identified lack of traceability as a significant threat. Traceability enables OEMs to deeply understand the security posture of their vehicles, enabling them to protect and maintain their vehicles from cybersecurity attacks. Without these critical elements of visibility and traceability, the millions of vehicles sold in 2021 will remain unprotected. Without traceability, there can be no visibility. Without visibility, it's near impossible to conduct risk assessment in a timely manner. In Europe alone, an estimated [1.] 21.3M vehicles will be sold in 2021 without basic cybersecurity foundation. Based on this statistic, over ten million vehicles will still be vulnerable to cyberattack. Because there is no full-spectrum visibility, manufacturers cannot design nor deploy proper cybersecurity protection. Moreover, without having a tool to monitor and knowledge to manage which vehicle models on the road have what hardware or software per electronic control unit (ECU) and their topology, manufacturers cannot maintain cybersecurity protection throughout the entire vehicle lifecycle.

”

21.3M vehicles will be sold in Europe in 2021 without basic cybersecurity foundation.

As has been established by these findings, deploying and maintaining in-vehicle cybersecurity is absolutely essential throughout the vehicle lifecycle. Without proper visibility, OEMs and Tier-1s are unable to gauge true cybersecurity needs and deploy relevant cybersecurity protection, leaving millions of vehicles vulnerable to attack.

”

Without proper visibility, OEMs and Tier-1s are unable to gauge true cybersecurity needs.

1. https://www.statista.com/statistics/640552/forecast-of-vehicle-sales-2021/

All rights reserved

RISK ASSESSMENT

Time is of the essence for risk assessment. How long does the typical risk assessment process take?

Risk assessment is one of the core activities professional cybersecurity teams need to conduct frequently. A rigid and efficient risk audit process forms the foundations for efficient automotive cybersecurity lifecycle management. The speed and depth with which an organization can perform these assessments is a quick win from a cybersecurity perspective: the faster a test can be run, the faster improvements can be put in place. However, approximately **56%** of survey participants estimate that the risk assessment process takes more than three weeks to manage - when the most effective risk assessment process should be near instantaneous.

> **The faster a test can be run, the faster improvements can be put in place.**

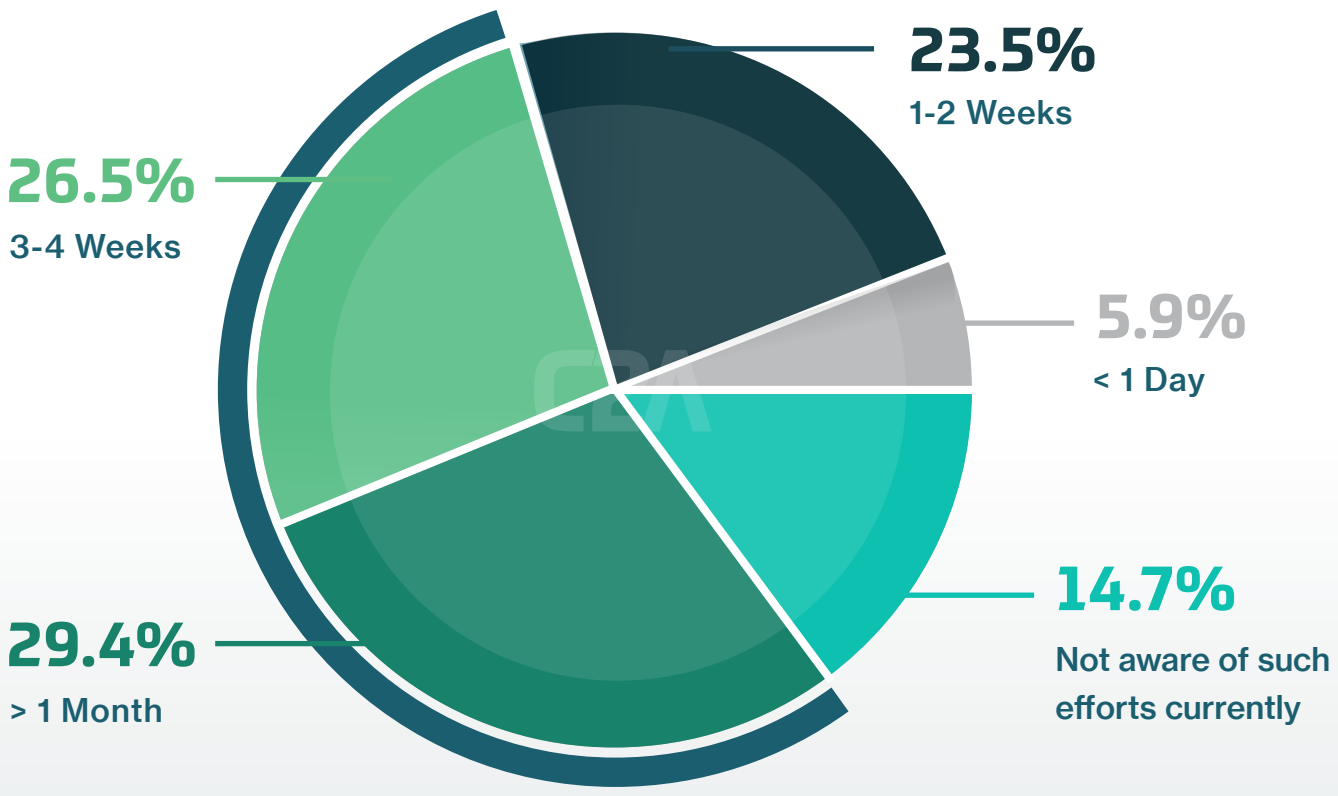
Fig B.

QUESTION:

How long does it take your organization to do risk assessment (New vulnerability is published)?

56%

estimate that the risk assessment process takes more than three weeks to manage



Looking at these findings, it's clear that most of the industry takes too long to identify risks and conduct risk assessments. Despite the fact that cybersecurity risk assessment happens periodically throughout the vehicle lifecycle, the industry is struggling to automate the process because it involves various events from multiple sources. As automotive attacks increase, so do the incidents that require urgent attention and resources.

All rights reserved

In the near future, automotive SOCs will be flooded with incidents on a daily basis. OEMs must have the ability to perform quick risk assessment, identify critical ones and mitigate them. Therefore, manufacturers will need to significantly up their reaction time to control and incident before it becomes a major, life-threatening issue. Such scenarios cannot be handled in the timeframe that most OEMs and Tier-1s are currently operating within.

As it stands, car companies don't have the ability to react to potential threats with urgency. With the implementation of digital solutions, effective risk assessment will not only be possible, but will quickly identify affected devices on an ongoing basis. A streamlined risk assessment process will enable OEMs to adapt to fast-emerging threats and vulnerabilities, reducing the time from weeks to hours, or even minutes, in the near future.

> **OEMs must have the ability to perform quick risk assessment, identify critical ones and mitigate them.**

There's room for improvement in the risk assessment process. The industry needs to ask: what's the hold up?

Communication and coordination between internal and external teams remains a point of contention in the risk assessment process, which has a direct impact on how long a typical risk assessment will take. The number of internal and external teams involved, location and time zones and the varying stages in the vehicle lifecycle are all factors that contribute to the delay. More than **50%** of participants indicate that coordination between the different entities is the biggest impediment to timely risk assessment process, followed by the lack of automation tools for each step (**35%**).

Fig C.

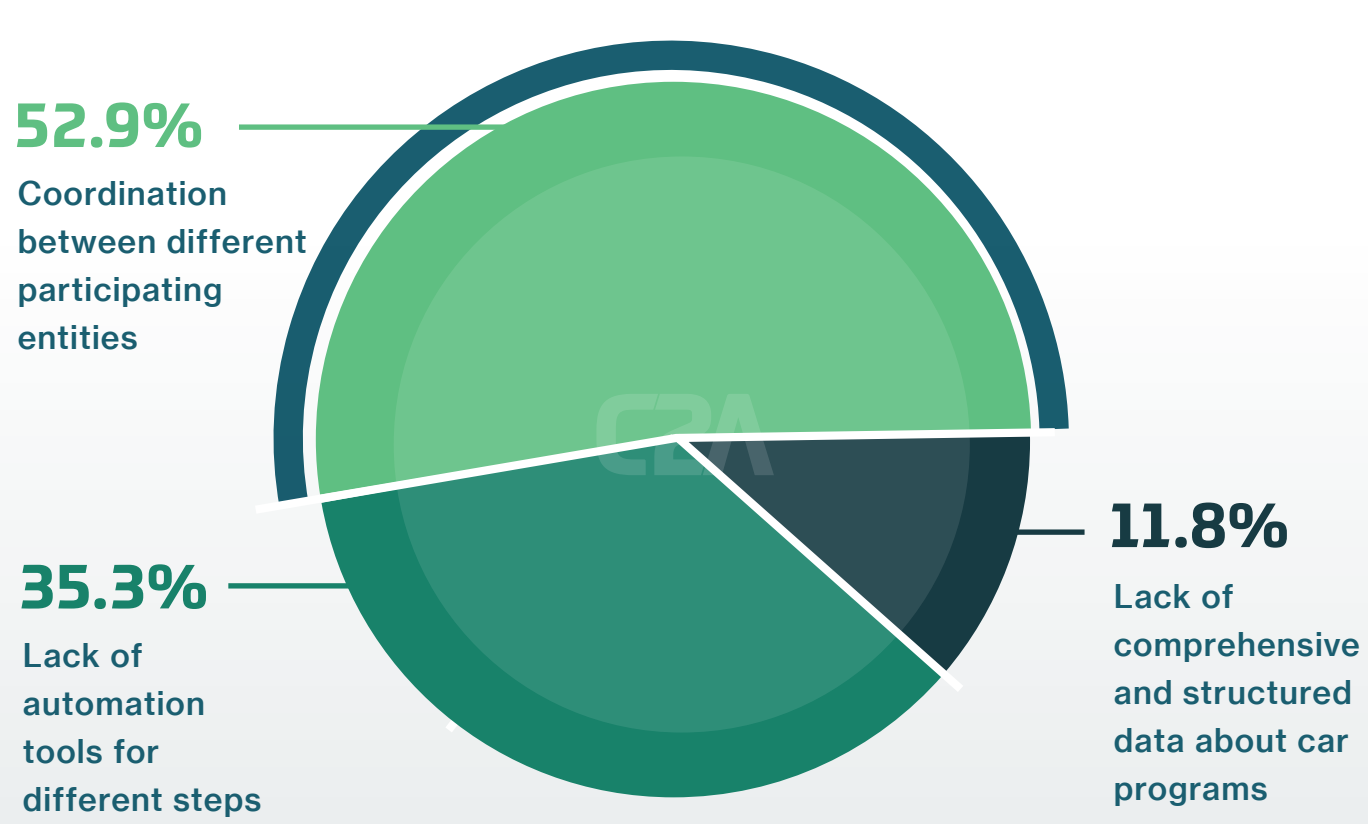
QUESTION:

What is the biggest impediment to timely risk assessment process?

Over

50%

of industry participnats agree that coordination between different participating entities poses the biggest risk to timley risk assessment process



All rights reserved

Collectively, these findings reveal an inextricable link between the effectiveness of the risk assessment process and the involvement of players in the supply chain. As risk assessment processes must account for all components of the vehicle, they should be performed throughout the supply chain to ensure the protection of pedestrians, drivers and passengers alike. A risk assessment process is not robust if it does not provide accurate, detailed insights into the cybersecurity posture of all components of vehicle architecture. It should enable pragmatic decision making, not cause more confusion in the process. Digitized tools and solutions to help streamline this process, which participants have a registered interest in, should be deployed to assist OEMs and suppliers to communicate information more freely and to perform cybersecurity quickly and more efficiently.

”

Digitized tools and solutions should be deployed to assist OEMs and suppliers to communicate information more freely.

Who should manage the risk assessment process?

It's widely agreed that OEMs should ultimately own the risk assessment process. As the vehicle manufacturer with ultimate responsibility towards the consumer and oversight over the supply chain, OEMs are best positioned to manage and conduct the risk assessment process throughout all phases of the cybersecurity lifecycle. This is particularly true in the case of cybersecurity risk audits and threat assessment and risk assessment (TARA), the foundation of each vehicle's cybersecurity goals and requirements.

Fig D.

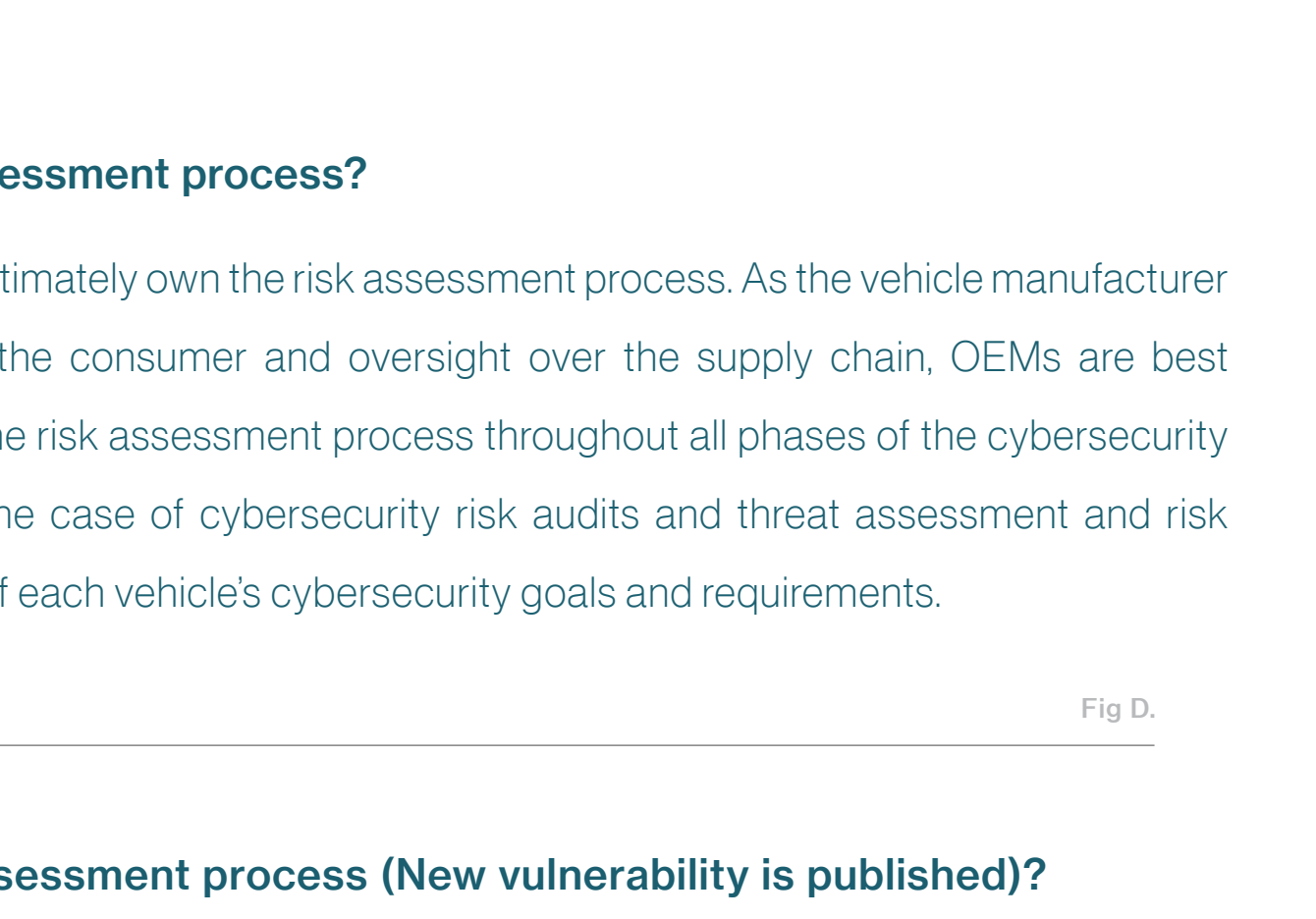
QUESTION:

Who should manage the risk assessment process (New vulnerability is published)?

Over than

70%

believe that the risk assessment process should be managed by each entity down the supply chain.



All rights reserved

However, survey results indicate that this is expanding. More than **70%** of participants believe that the risk assessment process should be managed by each entity down the supply chain. This represents a critical shift in thinking - cybersecurity is everyone's responsibility, and each entity should play its part in managing cybersecurity throughout the vehicle lifecycle. No OEM or supplier is solely in charge of cybersecurity lifecycle management; everyone is implicated and equally as responsible for the cybersecurity posture of the vehicle. With this new viewpoint, now is the time for the industry to establish harmonized communication between all entities down the supply chain, and create a uniform and effective channel for the risk assessment process that maintains in-vehicle cybersecurity throughout the vehicle lifecycle.

> **Cybersecurity is everyone's responsibility, and each entity should play its part in managing cybersecurity throughout the vehicle lifecycle.**

All rights reserved

Tackling ISO 21434 Policy Implementation

INDUSTRY CHALLENGES

The new regulations are a sign of maturity when it comes to cybersecurity lifecycle management. As ISO 21434 and UNECE WP.29 come into play, it's important to assess the readiness of OEMs, Tier-1s and suppliers to implement the policy in a way that will not only prevent disruption of cybersecurity management, but enhance existing cybersecurity management capabilities. Please note: "policy" in this section is synonymous with ISO 21434, and does not refer to internal cybersecurity policy.

What's your challenge?

> **62% OF SURVEY PARTICIPANTS RANKED COORDINATED IMPLEMENTATION ACROSS DIFFERENT TEAMS AND SUPPLIERS AS THE NUMBER ONE CHALLENGE IN ADDRESSING ISO 21434.**

Coordinating between the different internal and external teams responsible for implementing different aspects of the standard throughout the vehicle lifecycle poses a significant challenge for automotive manufacturers. There is a true need for an orchestration layer that streamlines the automotive manufacturers' management of all phases in the cybersecurity lifecycle: risk assessment, planning, policy creation and policy enforcement.

> **THE LACK OF CONCRETE IMPLEMENTATION STEPS AVAILABLE IS CAUSING CONFUSION AMONGST INDUSTRY LEADERS, SAY 36% OF PARTICIPANTS.**

The industry needs a feasible way to translate policies into each and every step of the security lifecycle. With no clear guidance on how to shift cybersecurity practices to be regulation-compliant, and lack of implementation processes for new ones, they could distract from building streamlined cybersecurity practices.

> **VISIBILITY OVER DIFFERENT CAR MODELS THROUGHOUT THE SECURITY LIFECYCLE STEPS IS A CORE CHALLENGE FOR 30% OF SURVEY RESPONDENTS.**

Gaining full spectrum visibility is critical for the successful implementation of ISO 21434. Guiding automotive manufacturers to implement cybersecurity management systems through visibility is one of the prerequisites to the concrete and effective implementation of ISO 21434.

All rights reserved

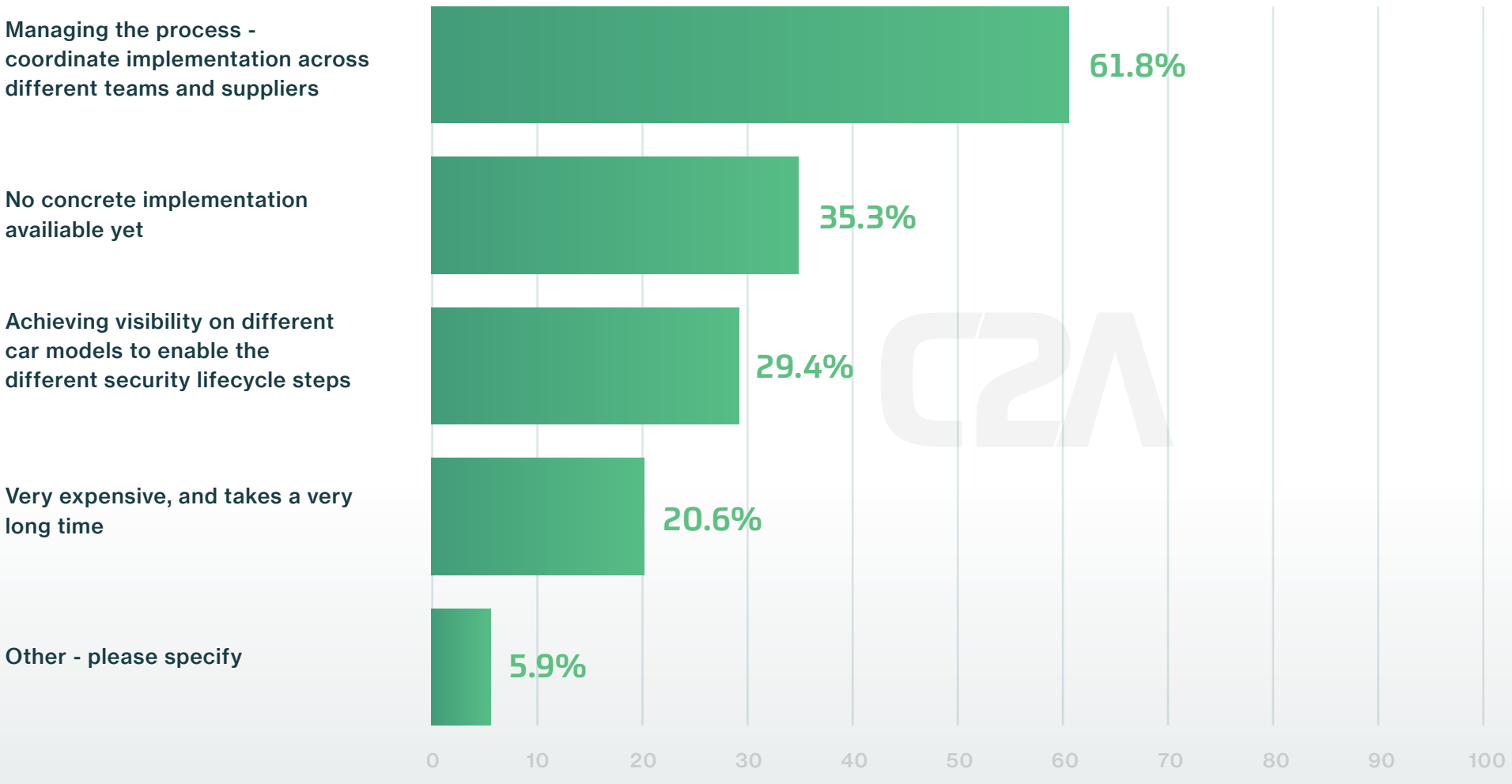
COST IS KEY FOR 21% OF PARTICIPANTS.

21% of participants pointed to cost as the main challenge in adopting ISO 21434 regulations, a very expensive process that takes a significant amount of time and resources, mostly because OEMs lack the proper means and automated tools to achieve efficiency during the implementation process. The cost factor is even more important when considering the average vehicle is on the road for over two decades, and thus will need to remain cybersecurity compliant for that time.

Fig E.

QUESTION:

What are your main challenges to adopt the ISO 21434 standard througout the vehicle lifecycle (not only until production)? Please mark all relevant answers



These four key challenges prove that there are a variety of factors that contribute to proper automotive cybersecurity posture, particularly when it comes to implementing new regulations. A streamlined cybersecurity lifecycle management process is needed to support companies as they begin to implement the new standard.

> **Streamlined cybersecurity lifecycle management process is needed to support companies as they begin to implement the new standard.**

All rights reserved

CONCLUSION

The automotive industry is in the midst of an upheaval: as automakers struggle with connected vehicle architecture, new standards, regulations and a fragmented supply chain, an opportunity has emerged to transform archaic approaches to cybersecurity lifecycle management into digital solutions that provide visibility and control throughout the vehicle lifecycle. With new solutions, the industry can better manage modern vehicle architecture, significantly speed up the reaction to attacks for the entire supply chain and better collaborate to implement an ISO 21434 framework, and other regulations for the future.

Findings have only reinforced that visibility and traceability are essential to the implementation of ISO 21434, in performing accurate and fast risk assessment processes and to deploy and maintain protection of automotive cybersecurity. Furthermore, the supply chain is in desperate need for harmonized communication that will enable all parties to speak the same language and tackle problems efficiently, and as one entity. All of this can be enabled with automation and digitization, which should have a larger share in dealing with cybersecurity needs of connected cars.

> **”**
>
> **With new solutions, the industry can better manage modern vehicle architecture, significantly speed up the reaction to attacks and better collaborate to implement ISO 21434 framework.**

This opportunity is one that should be taken now, and with urgency. Armed with visibility, the industry will be able to come together to streamline cybersecurity lifecycle management to bring safer vehicles to the road for drivers, passengers and pedestrians alike.

All rights reserved

APPENDIX A - METHODOLOGY

COLLECTION METHODOLOGY

C2A Security conducted the survey through direct outreach to industry stakeholders. The company identified a number of organizations, key thought leaders and specialists to target so as to diversify perspectives reflected in the results and capture a balanced assessment of the state of the industry. In exchange for responding to the survey, participants received early access to findings and market reports. The findings reflect the point of view of professionals working for OEMs as well as Tier-1 companies.

THE SURVEY

The survey consisted of a combination of yes and no, timeline and qualitative questions:

A. Visibility and transparency

> Do you have a complete HW & SW BOM visibility of your car models (starting next year)?

> Do you have traceability from SW & HW BOM to VIN number (which vehicle on the road has what HW/SW per ECU)?

B. Risk Assessment

> When a new vulnerability is published, who should manage the risk assessment process?
>
> **A.** The OEM
>
> **B.** The suppliers
>
> **C.** Each entity, down the supply chain

> When a new vulnerability is published, how long does it take your organization to do risk assessment?
>
> **A.** Not aware of such efforts currently
>
> **B.** > 1 Month
>
> **C.** 3-4 Weeks
>
> **D.** 1-2 Weeks
>
> **E.** < 1 Day

All rights reserved

What is the biggest impediment to timely risk assessment process?

A. Lack of comprehensive and structured data about car programs

B. Lack of automation tools for different steps

C. Coordination between different participating entities

C. Policy Implementation

What are your main challenges to adopt the ISO 21434 standard throughout the vehicle lifecycle (not only until production)?

A. No concrete implementation available yet

B. Managing the process - coordinate implementation across different teams and suppliers

C. Achieving visibility on different car models to enable the different security lifecycle steps

D. Very expensive, and takes a very long time

E. Other - please specify

Do you have any additional comments on the challenges in executing comprehensive security lifecycle management?

All rights reserved

ABOUT C2A SECURITY

C2A Security is a trusted end-to-end automotive cybersecurity solutions provider. Its suite of embedded cybersecurity solutions takes a multi-layered approach to provide automotive-relevant protection and safety compatibility. With market neutrality, complete fluency in the needs of the automotive industry and ease of integration, C2A is redefining the automotive cybersecurity ecosystem. C2A is the sole provider of the most flexible, comprehensive and transparent cybersecurity solutions on the market. For more information, visit www.c2a-sec.com